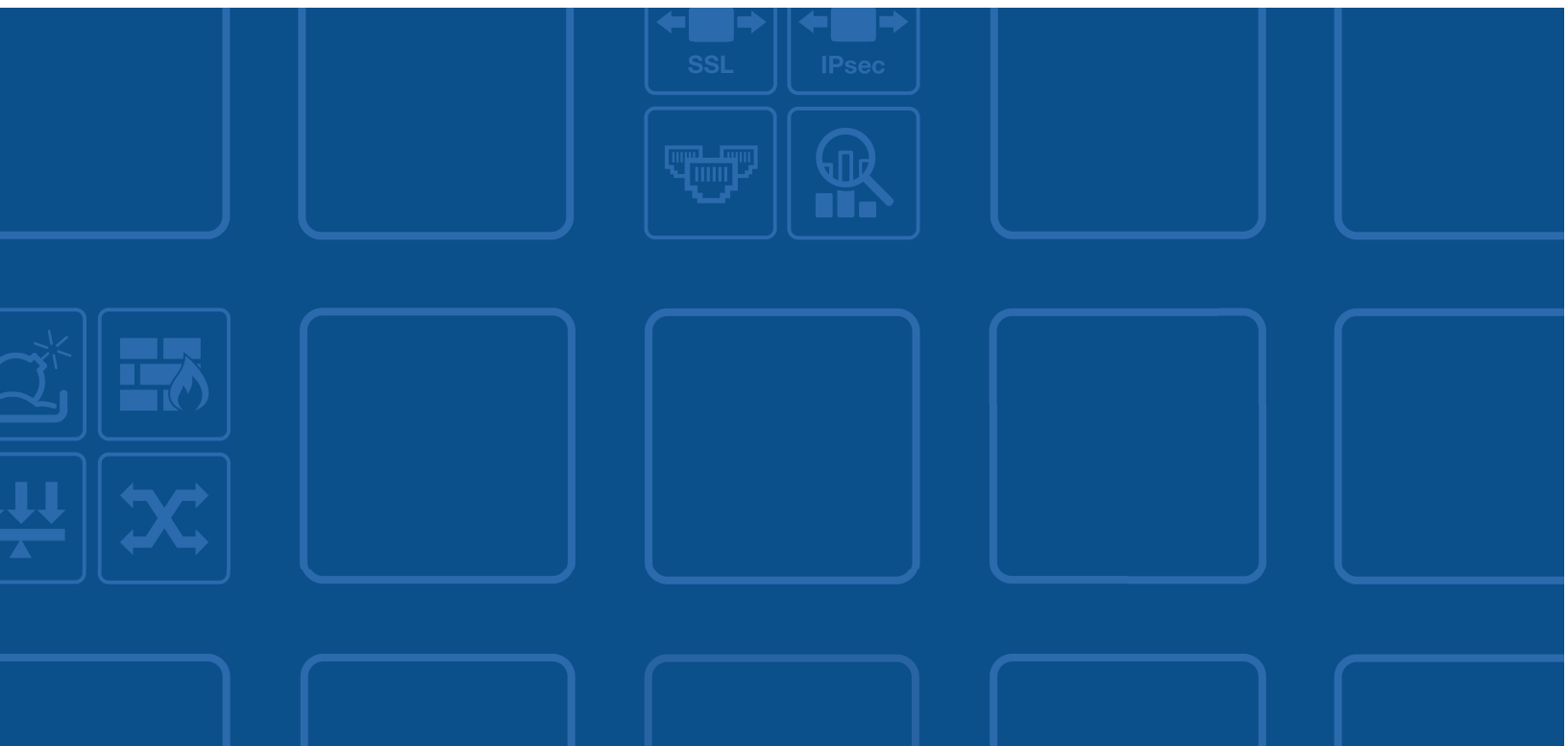
FORTINET
High Performance Network Security

# FortiOS - Release Notes

VERSION 5.2.9



**FORTINET DOCUMENT LIBRARY**

http://docs.fortinet.com

**FORTINET VIDEO GUIDE**

http://video.fortinet.com

**FORTINET BLOG**

https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**

https://support.fortinet.com

**FORTIGATE COOKBOOK**

http://cookbook.fortinet.com

**FORTINET TRAINING SERVICES**

http://www.fortinet.com/training

**FORTIGUARD CENTER**

http://www.fortiguard.com

**END USER LICENSE AGREEMENT**

http://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**

Email: techdocs@fortinet.com

March 22, 2017

FortiOS 5.2.9 Release Notes

01-529-384208-20170322

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
|---|---|
| 2016-09-07 | Initial release. |
| 2016-09-08 | Moved 379870 from Known Issues to Resolved Issues. |
| 2016-09-12 | Added 289773 to Resolved Issues. |
| 2016-09-15 | Added 287871 to Known Issues, added *Local report customization removed* to Special Notices, moved 374283 to the Anti-spam table within Resolved Issues, and added info about web filter log options to Upgrade Information. |
| 2016-09-21 | Added 388032 to Known Issues. |
| 2016-10-03 | Added 381168 to Resolved Issues. |
| 2016-10-24 | Removed 267957 from Known Issues > GUI. |
| 2016-11-17 | Added 373707 to Resolved Issues. |
| 2016-11-21 | Updated build number for the following models: FG-5001B, FG-5001C, FG-5001D, FG-5101C. Added FG-5000 Series section to Resolved Issues. |
| 2016-11-29 | Updated support for FortiSwitch OS (FortiLink support) |
| 2017-03-22 | Removed *273910* from *Known Issues*. |

# Introduction

This document provides the following information for FortiOS 5.2.9 build 0736:

- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- Limitations

See the Fortinet Document Library for FortiOS documentation.

## Supported models

FortiOS 5.2.9 supports the following models.

| | |
|---|---|
| **FortiGate** | FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-SFP, FG-60C-POE, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FGT-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG- 111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG- 200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-310B-DC, FG-311B, FG-400D, FG-500D, FG-620B, FG-620B-DC, FG- 621B, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3040B, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810D, FG-3815D, FG-3950B, FG-3951B |
| **FortiWiFi** | FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D |
| **FortiGate Rugged** | FGR-60D, FGR-100C |
| **FortiGate VM** | FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN |
| **FortiSwitch** | FS-5203B |
| **FortiOS Carrier** | FCR-3950B and FCR-5001B<br>FortiOS Carrier 5.2.9 images are delivered upon request and are not available on the customer support firmware download page.<br><br>FortiOS Carrier firmware image file names begin with *FK*. |

The following models are released on a special branch based off of FortiOS 5.2.9. As such, the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays the build number.

| | |
|---|---|
| **FGT-VM64-AWS/AWSONDEMAND** | Released on build 9259. |
| **FGT-VM64-AZURE** | Released on build 5613. |
| **FG-5001B** | Released on build 5788. |
| **FG-5001C** | Released on build 5788. |
| **FG-5001D** | Released on build 5788. |
| **FG-5101C** | Released on build 5788. |

To confirm that you are running the proper build, the output from the `get system status` CLI command has a **branch point field** that should read 0736.

The FG-60D-3G4G-VZW model uses the FGT_60D_MC-v5-build0736-FORTINET.out image. The FWF-60D-3G4G-VZW model uses the FWF_60D_MC-v5-build0736-FORTINET.out image.

## Last Release of Software

Due to the device flash size limitations, the following FortiGate models' last release of software will be FortiOS version 5.2.5. It is noted that these devices already have entered into their End-of-Life Cycle. Further details and exact dates can be found on the Fortinet Customer Support portal:

**Affected Products:**

- FortiGate FG-3016B
- FortiGate FG-3810A
- FortiGate FG-5001A SW & DW
- FortiCarrier FK-3810A
- FortiCarrier FK-5001A SW & DW

# Special Notices

## Local report customization removed

Local report customization has been removed from FortiOS 5.2. You can still record and view local reports, but you can no longer customize their appearance. For more control over customizing local reports, you can use FortiAnalyzer or FortiCloud.

## Compatibility with FortiOS versions

The following units have a new WiFi module built-in that is not compatible with FortiOS 5.2.1 and lower. It is recommended to use FortiOS 5.2.2 and later for these units.

**Affected models**

| Model | Part Number |
|---|---|
| FWF-60CX-ADSL | PN: 8918-04 and later |

The following units have a memory compatibility issue with FortiOS 5.2.1 and lower. It is recommended to use FortiOS 5.2.2 and later for these units.

**Affected models**

| Model | Part Number |
|---|---|
| FG-600C | PN: 8908-08 and later |
| FG-600C-DC | PN: 10743-08 and later |
| FG-600C-LENC | PN: 11317-07 and later |

## Removed WANOPT, NETSCAN, FEXP features from USB-A

The following features have been removed from the FortiGate and FortiWiFi 80C, 80CM, and 81CM:

- WAN Optimization
- Vulnerability scanning
- Using FortiExplorer on a smartphone to manage the device by connecting to the USB-A port

## Router Prefix Sanity Check

Prior to FortiOS 5.2.4 under the config router prefix table, if there are any `le` and `ge` settings that have the same prefix length as the prefix, you may lose the prefix rule after upgrading to FortiOS 5.2.4 or later.

## WAN Optimization in FortiOS 5.2.4

In FortiOS 5.2.4:

- If your FortiGate does not have a hard disk, WAN Optimization is not available.
- If your FortiGate has a hard disk, you can configure WAN Optimization from the CLI.
- If your FortiGate has two hard disks, you can configure WAN Optimization from the GUI.

See the FortiOS 5.2.4 Feature Platform Matrix to check the availability for your FortiGate model.

## Built-In Certificate

FortiGate and FortiWiFi D-series and above have a built in Fortinet_Factory certificate that uses a 2048-bit certificate with the 14 DH group.

## FortiGate-92D High Availability in Interface Mode

The FortiGate-92D may fail to form an HA cluster and experience a spanning tree loop if it is configured with the following:

- operating in interface mode
- at least one of the interfaces, for example *interface9*, is used has the HA heartbeat interface
- a second interface is connected to an external switch

Workaround: use either WAN1 or WAN2 as the HA heartbeat device.

## Default log setting change

For FG-5000 blades and FG-3900 series, log disk is disabled by default. It can only be enabled via CLI. For all 2U & 3U models (FG-3600/FG-3700/FG-3800), log disk is also disabled by default. For all 1U models and desktop models that supports SATA disk, log disk is enabled by default.

## FG-5001D operating in FortiController or Dual FortiController mode

When upgrading a FG-5001D operating in FortiController or dual FortiController mode from version 5.0.7 (B4625) to FortiOS version 5.2.3, you may experience a back-plane interface connection issue. This is due to a change to

the ELBC interface mapping ID. After the upgrade, you will need to perform a factory reset and then re-configure the device.

## FortiGate units running 5.2.9

FortiGate units running 5.2.9 and managed by FortiManager 5.0.0 or 5.2.0 may report installation failures on newly created VDOMs, or after a factory reset of the FortiGate unit even after a retrieve and re-import policy.

For the latest information, see the FortiManager and FortiOS Compatibility.

## Firewall services

Downgrading from 5.2.3 to 5.2.2 may cause the default protocol number in the firewall services to change. Double check your configuration after downgrading to 5.2.2.

## FortiPresence

For FortiPresence users, it is recommended to change the FortiGate web administration TLS version in order to allow the connection.

```
config system global
   set admin-https-ssl-versions tlsv1-0 tlsv1-1 tlsv1-2
end
```

## SSL VPN setting page

The default server certificate has been changed to the `Fortinet_Factory` option. This excludes FortiGate-VMs which remain at the `self-signed` option. For details on importing a CA signed certificate, please see the How to purchase and import a signed SSL certificate document.

# Upgrade Information

## Upgrading from FortiOS 5.2.6 or later

FortiOS version 5.2.9 officially supports upgrade from version 5.2.6 or later.

## Upgrading from FortiOS 5.0.12 or later

FortiOS version 5.2.9 officially supports upgrade from version 5.0.12 or later.

When upgrading from a firmware version beyond those mentioned in the Release Notes, a recommended guide for navigating the upgrade path can be found on the Fortinet documentation site.

There is separate version of the guide describing the safest upgrade path to the latest patch of each of the supported versions of the firmware. To upgrade to this build, go to FortiOS 5.2 Supported Upgrade Paths

### Web filter log options change from disabled to enabled after upgrade

After upgrading from FortiOS 5.0.12 or 5.0.14 to FortiOS 5.2.9, all log options for web filter change from disabled to enabled, except the `log-all-url` option.

## Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles.

# FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

**Citrix XenServer and Open Source XenServer**

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

**Linux KVM**

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

**Microsoft Hyper-V**

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

**VMware ESX and ESXi**

- `.out`: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 32-bit or 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

# Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

# Product Integration and Support

## FortiOS 5.2.9 support

The following table lists 5.2.9 product integration and support information:

| | |
|---|---|
| **Web Browsers** | • Microsoft Internet Explorer version 11<br>• Mozilla Firefox version 42<br>• Google Chrome version 46<br>• Apple Safari version 7.0 (For Mac OS X)<br>Other web browsers may function correctly, but are not supported by Fortinet. |
| **Explicit Web Proxy Browser** | • Microsoft Internet Explorer versions 8, 9, 10, and 11<br>• Mozilla Firefox version 27<br>• Apple Safari version 6.0 (For Mac OS X)<br>• Google Chrome version 34<br>Other web browsers may function correctly, but are not supported by Fortinet. |
| **FortiManager** | For the latest information, see the FortiManager and FortiOS Compatibility.<br><br>You should upgrade your FortiManager prior to upgrading the FortiGate. |
| **FortiAnalyzer** | For the latest information, see the FortiAnalyzer and FortiOS Compatibility.<br><br>You should upgrade your FortiAnalyzer prior to upgrading the FortiGate. |
| **FortiClient Microsoft Windows and FortiClient Mac OS X** | • 5.4.0 and later<br>• 5.2.5 and later |
| **FortiClient iOS** | • 5.4.1<br>• 5.2.2 and later |
| **FortiClient Android and FortiClient VPN Android** | • 5.2.8<br>• 5.2.7 |

| | |
|---|---|
| **FortiAP** | • 5.2.5 and later<br>• 5.0.10<br>You should verify what the current recommended FortiAP version is for your FortiAP prior to upgrading the FortiAP units. You can do this by going to the *WiFi Controller* > *Managed Access Points* > *Managed FortiAP* page in the GUI. Under the *OS Version* column you will see a message reading *A recommended update is available* for any FortiAP that is running an earlier version than what is recommended. |
| **FortiSwitch OS (FortiLink support)** | • 3.4.2 build 0192<br>Supported models: all FortiSwitch D models. |
| **FortiSwitch-ATCA** | • 5.0.3 and later<br>Supported models: FS-5003A, FS-5003B |
| **FortiController** | • 5.2.0 and later<br>Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C<br>• 5.0.3 and later<br>Supported model: FCTL-5103B |
| **FortiSandbox** | • 2.2.1<br>• 2.1.0 |
| **Fortinet Single Sign-On (FSSO)** | • 5.0 build 0251 (needed for FSSO agent support OU in group filters)<br>  • Windows Server 2008 (64-bit)<br>  • Windows Server 2008 R2 64-bit<br>  • Windows Server 2012 Standard<br>  • Windows Server 2012 R2 Standard<br>  • Novell eDirectory 8.8<br>• 4.3 build 0164 (contact Support for download)<br>  • Windows Server 2003 R2 (32-bit and 64-bit)<br>  • Windows Server 2008 (32-bit and 64-bit)<br>  • Windows Server 2008 R2 64-bit<br>  • Windows Server 2012 Standard Edition<br>  • Windows Server 2012 R2<br>  • Novell eDirectory 8.8<br>FSSO does not currently support IPv6. |
| **FortiExplorer** | • 2.6 build 1083 and later.<br>Some FortiGate models may be supported on specific FortiExplorer versions. |
| **FortiExplorer iOS** | • 1.0.6 build 0130 and later<br>Some FortiGate models may be supported on specific FortiExplorer iOS versions. |

| | |
|---|---|
| **FortiExtender** | • 3.0.0 build 0069<br>• 2.0.0 build 0003 and later |
| **AV Engine** | • 5.177 |
| **IPS Engine** | • 3.170 |
| **Virtualization Environments** | |
| **Citrix** | • XenServer version 5.6 Service Pack 2<br>• XenServer version 6.0 and later |
| **Linux KVM** | • RHEL 7.1/Ubuntu 12.04 and later<br>• CentOS 6.4 (qemu 0.12.1) and later |
| **Microsoft** | • Hyper-V Server 2008 R2, 2012, and 2012 R2 |
| **Open Source** | • XenServer version 3.4.3<br>• XenServer version 4.1 and later |
| **VMware** | • ESX versions 4.0 and 4.1<br>• ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5 and 6.0 |

## Language support

The following table lists language support information.

**Language support**

| Language | GUI |
|---|---|
| English | ✓ |
| Chinese (Simplified) | ✓ |
| Chinese (Traditional) | ✓ |
| French | ✓ |
| Japanese | ✓ |
| Korean | ✓ |
| Portuguese (Brazil) | ✓ |
| Spanish (Spain) | ✓ |

# SSL VPN support

## SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

**Operating system and installers**

| Operating System | Installer |
|---|---|
| Microsoft Windows XP SP3 (32-bit)<br>Microsoft Windows 7 (32-bit & 64-bit)<br>Microsoft Windows 8 (32-bit & 64-bit)<br>Microsoft Windows 8.1 (32-bit & 64-bit) | 2328 |
| Microsoft Windows 10 (32 bit & 64 bit) | 2329 |
| Linux CentOS 6.5 (32-bit & 64-bit)<br>Linux Ubuntu 12.0.4 (32-bit & 64-bit) | 2328 |
| Virtual Desktop for Microsoft Windows 7 SP1 (32-bit) | 2328 |

Other operating systems may function correctly, but are not supported by Fortinet.

## SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

**Supported operating systems and web browsers**

| Operating System | Web Browser |
|---|---|
| Microsoft Windows 7 SP1 (32-bit) | Microsoft Internet Explorer versions 9, 10 and 11<br>Mozilla Firefox version 33 |
| Microsoft Windows 7 SP1 (64-bit) | Microsoft Internet Explorer versions 9, 10, and 11<br>Mozilla Firefox version 33 |
| Microsoft Windows 8/8.1 (32bit/62bit) | Microsoft Internet Explorer versions 10 and 11<br>Mozilla Firefox 42 |
| Mac OS 10.9 | Safari 7 |
| Linux CentOS version 5.6 | Mozilla Firefox version 5.6 |
| Linux Ubuntu version 12.0.4 | Mozilla Firefox version 5.6 |

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

## SSL VPN host compatibility list

The following table lists the antivirus and firewall client software packages that are supported.

**Supported Microsoft Windows XP antivirus and firewall software**

| Product | Antivirus | Firewall |
|---|---|---|
| Symantec Endpoint Protection 11 | ✓ | ✓ |
| Kaspersky Antivirus 2009 | ✓ | |
| McAfee Security Center 8.1 | ✓ | ✓ |
| Trend Micro Internet Security Pro | ✓ | ✓ |
| F-Secure Internet Security 2009 | ✓ | ✓ |

**Supported Microsoft Windows 7 32-bit antivirus and firewall software**

| Product | Antivirus | Firewall |
|---|---|---|
| CA Internet Security Suite Plus Software | ✓ | ✓ |
| AVG Internet Security 2011 | | |
| F-Secure Internet Security 2011 | ✓ | ✓ |
| Kaspersky Internet Security 2011 | ✓ | ✓ |
| McAfee Internet Security 2011 | ✓ | ✓ |
| Norton 360™ Version 4.0 | ✓ | ✓ |
| Norton™ Internet Security 2011 | ✓ | ✓ |
| Panda Internet Security 2011 | ✓ | ✓ |
| Sophos Security Suite | ✓ | ✓ |
| Trend Micro Titanium Internet Security | ✓ | ✓ |
| ZoneAlarm Security Suite | ✓ | ✓ |
| Symantec Endpoint Protection Small Business Edition 12.0 | ✓ | ✓ |

# Resolved Issues

The following issues have been fixed in version 5.2.9. For inquires about a particular bug, please contact Customer Service & Support.

### FG-5000 Series

| Bug ID | Description |
|---|---|
| 391109 | An SLBC cluster may fail to upgrade all units in the cluster. |
| 388046 | The `confsyncd` daemon may leak memory. |
| 384698 | Cache memory usage may increase abruptly. |
| 387118 | Slave FG-5001C failed to synchronize the WAN Opt storage size. |

### Antivirus

| Bug ID | Description |
|---|---|
| 289773 (duplicate of 378521) | FTP active mode connection fails on getting virus files. |

### DLP

| Bug ID | Description |
|---|---|
| 369825 | There exists inconsistent DLP behavior. |

### Firewall

| Bug ID | Description |
|---|---|
| 375678 | Update-all-session-timer may not work as expected. |
| 370201 | IMD may crash when unregistering SIP with asterisk (*) contact, or multiple REGISTER messages with the same AOR and multiple contacts |
| 368838 | Active-flow-timeout does not take effect on the http protocol when NP6 is offloaded. |
| 297421 | HTTPs traffic is blocked after AV/IPS database update from FortiGuard. |
| 227034 | Inaccurate netflow report. |

### GUI

| Bug ID | Description |
|---|---|
| 286533 | Should respect use-management-vdom setting when testing RADIUS connectivity. |
| 269191 | Client monitor page does not show clients when the filter is set on SSID. |

### High Availability

| Bug ID | Description |
|---|---|
| 378213 | After a reboot of the FGT that holds the SCTP secondary path, the session is missing and will be reopened with delay. |
| 376449 | Traffic packets were not counted on the master session after path failover, which causes the master session to be removed after timeout. |
| 374990 | Extended Sequence Number issue in HA firewalls. |
| 374272 | NTP keeps using VDOM root to sync when HA standalone-mgmt-vdom is enabled. |
| 368447 | 3FGSP should not sync static BFD setting. |

### IPS

| Bug ID | Description |
|---|---|
| 371254 | Ipsengine signal 11 crash happens on FWF_90D when IPS custom signature is detected. |

### IPv6

| Bug ID | Description |
|---|---|
| 376452 | ICMPv6 "Time Exceeded" packets are not forwarded when the original ICMPv6 packet has the "Hop-by-Hop" option. |

### Logging & Report

| Bug ID | Description |
|---|---|
| 377928 | FortiCloud report may not display on low-end platforms without SSD. |
| 306929 | Fortigate memory logging is automatically enabled after reboot. |

### Routing

| Bug ID | Description |
|---|---|
| 369864 | BFD is DOWN randomly. |

### SSL VPN

| Bug ID | Description |
|---|---|
| 382828 | When trying to access internal server through SSL VPN in web mode, the login page is not displayed, while in tunnel-mode it works. |
| 379450 | Sslvpn crashes with segmentation fault in 'sslvpn_ap_table_get' after upgrading to 5.4.1. |
| 371264 | Modify user ran into lock when trying to change user's password during sslvpn connection. |
| 243643 | "Modified Date" SMB does not match the actual file dates on SMB Server |

### System

| Bug ID | Description |
|---|---|
| 380964,378420 | FortiGate port flapping causes HA fail over on 3X40B and 395XB. |
| 380161 | No reply to SNMP queries if reply should be routed via PBR. |
| 376599 | Keep IPSec traffic on the hardware during rekeying causes kernel panic. |
| 375141 | The ips view ID is incorrect when the ID is greater than 4096 and NTurbo is enabled on NP6. |
| 374720, 379637 | Kernel NULL pointer dereference. |
| 373820 | Snmpwalk to "ipRouteTable" takes too long if there is a large number of routes in the routing table. |
| 371194 | After the CRL is updated by ldap-server, http-url, or scep-url, admin can change the CRL content, which may confuse users as well as fail FortiManager config installation and verification. |
| 308693 | Setting cfg-save to manual or revert causes NAT to be disabled and Security Profiles to be removed when editing the policy via GUI. |
| 295508 | PPPoE connection is unstable and cannot recover automatically. |
| 292615 | Vlan interface based on NPU vdom link cannot be displayed on the vdom-network-interface page. |

| Bug ID | Description |
|---|---|
| 284936 | Malformed SNMP v2c packets are generated when the interface IP is changed. |
| 282472 | NP6 multicast traffic is duplicated. |

### WiFi

| Bug ID | Description |
|---|---|
| 381030 | WPA-Personal passphrase should support a fixed-length of 64 hexadecimal digits. |
| 365255 | FWF-60D kernel panic happened with message "unexpected multicast address". |
| 240602 | Anonymous identity should not replace the real authentication account when users connect using WPA-Enterprise. |

### Common Vulnerabilities and Exposures

| Bug ID | Description |
|---|---|
| 383564 | FortiOS 5.2.9 is no longer vulnerable to the following CVE Reference:<br>• 2016-5696<br>Visit https://fortiguard.com/psirt for more information. |
| 378697 | FortiOS 5.2.9 is no longer vulnerable to the following CVE Reference:<br>• 2016-2512<br>Visit https://fortiguard.com/psirt for more information. |
| 379870 | FortiOS 5.2.9 is no longer vulnerable to the following CVE References:<br>• 2003-1418<br>• 2007-6750<br>Visit https://fortiguard.com/psirt for more information. |
| 381168 | FortiOS 5.2.9 is no longer vulnerable to the following CVE Reference:<br>• 2004-0230<br>Visit https://fortiguard.com/psirt for more information. |
| 373707 | FortiOS 5.2.9 is no longer vulnerable to the following CVE Reference:<br>• 2016-1550<br>Visit https://fortiguard.com/psirt for more information. |

# Known Issues

The following issues have been identified in version 5.2.9. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

### Anti-spam

| Bug ID | Description |
|---|---|
| 374283 | Spamfilter does not leave Anti-Spam log for the exempted traffic by bwl matching. |

### FortiGate 3810D

| Bug ID | Description |
|---|---|
| 285429 | Traffic may not be able to go through the NPU VDOM link with traffic sharper enabled on FortiGate-3810D TP mode. |

### FortiGate 3815D

| Bug ID | Description |
|---|---|
| 385860 | FGT-3815D does not support 1GE SFP transceivers. |

### FortiGate-VM

| Bug ID | Description |
|---|---|
| 272438 | During the boot-up sequence, the FortiGate-VM device may encounter a harmless configuration error message. |

### FortiSandbox

| Bug ID | Description |
|---|---|
| 273244 | On the FortiGate device in *FortiView* > *FortiSandbox*, the analysis result may show a pending status and the FortiCloud side may show an unknown status. |
| 269830 | The UTM log may incorrectly report a file that has been sent to FortiSandbox. *FortiView* > *FortiSandbox* may still show files are submitted even after the daily upload quota has been reached. |

### FortiSwitch

| Bug ID | Description |
|---|---|
| 376375 | FSW with B0181 (v3.4.1) can be discovered but may not be able to obtain the `IP addr` and be authorized successfully. |

### GUI

| Bug ID | Description |
|---|---|
| 310930 | LDAP browser in `LDAP-group-GUI` may not respect group filter from LDAP server. |
| 286226 | Users may not be able to create new address objects from the Firewall Policy. |
| 285813 | When navigating `FortiView > Application` some security action filters may not work. |
| 278638 | Explicit policy may be automatically reset to log security events. |
| 271113 | When creating an `id_based policy` with SSL enabled, and the set `gui-multipleutm disable` is applied, an *Entry not found* error message may appear. |
| 268346 | *All sessions: filter application*, *threat*, and *threat type*, may not work as expected |
| 246546 | Adding an override application signature may cause all category settings to be lost. |
| 215890 | Local-category status display may not change after running `unset category-override` in the CLI. |

### System

| Bug ID | Description |
|---|---|
| 302272 | Medium type may be shown incorrectly on shared ports. |
| 285981 | Adding more than eight members to `LACP get np6_lacp_add_slave` may result in an error. |
| 285520 | On NP4 platforms, TCP traffic may not be able to be offloaded in the decryption direction. |
| 263864 | When the interface is configured with *Auto-Speed*, FG-3240C NP4 Port 1G may stay down after reboot.<br>**Workaround**: Set the interface speed to *1000/Full*. |
| 287871 | Administrative HTTPS and SSLVPN access using second WAN interface does not work after upgrade to 5.2.9. |

| Bug ID | Description |
|---|---|
| 388032 | Corrupted packets may cause malfunction of NP6, which causes NP ports to be unable to accept and forward traffic.<br>**Affected models**: All NP6 platforms. |

### VoIP

| Bug ID | Description |
|---|---|
| 272278 | SIP calls may be denied when using a combination of SIP ALG, IPS, and AppCtrl. |

### Webfilter

| Bug ID | Description |
|---|---|
| 380119 | Webfilter static URL filter blocks additional domains with similar names. |
| 378277 | YouTube header injection (replacement for YouTube for Schools) was deleted. |
| 377753 | Modify antispam logic to handle `local-override`. |
| 284661 | If the requested URL has port number, the URL filter may not block properly. |

### WiFi

| Bug ID | Description |
|---|---|
| 267904 | If the client is connecting to an SSID with WPA-Enterprise and User-group, it may not be able to pass the traffic policy. |
| 355335 | SSID may stop broadcasting. |

# Limitations

## Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

## Open Source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

FORTINET®

*High Performance Network Security*